REPLACEMENT SPECIFICATION

BACKGROUND OF THE INVENTION

The invention relates to a method for secure data transmission in selling products in stores. These stores contain a product selection terminal as well as a counter means having a document reading station, and a product delivery storage system in which a product is selected at the product selection terminal and a document for the selected product is output by means of a printer device.

In purchasing products and especially products with higher costs or quality, the selection and the delivery of the products being handled in different areas of the store require a counterfeit-proof means of_transmission of the product data starting at the detection and up to the authorized product delivery.

DE 42 17 045 A1 teaches a method for selling products in which the products are stored in an automatic delivery apparatus and in which at least one product delivery terminal, as well as a counter, are provided. In selecting the products at the product selection terminal, a signal specifically for the selection is generated. After the payment of the product value, the counter generates a purchase document which is supplied to a reading device of the automatic delivery apparatus and which causes the delivery of the corresponding product from the automatic delivery apparatus.

Further, DE 695 04 729 T2 which is a translation of EP 0 670 132 B1 teaches an apparatus for providing packs of cigarettes at a plurality of cash desks wherein the apparatus comprises a central store room as well as a means set up on the cash desk and capable of performing a selection of the kind of packs, and a transport system for supplying the packs to the cash desk

The known methods have the disadvantage of either that expensive transport systems are needed or the purchase documents offer insufficient security against improper use especially for high cost or quality products.

SUMMARY OF THE INVENTION

It is therefore an object of the invention to provide a method of providing secure transmission of information about purchased products in a store, such that one or more documents and information carriers for product identification, respectively, are provided with measures protected against copying and ensuring an authorized product delivery.

This object is achieved by the fact that the document is provided with a first self-checking encryption code and with a first algorithm for encrypting a product identification of the selected product or the selling identification of a selling process. Additionally one or more selling identifications are provided on said document, and the encryption on said document is identified (decrypted) at the document reading station. The value associated to said product is detected at the document reading station and forwarded to said counter means for balancing the value (payment). After the payment of said product, said counter means delivers an electronic information carrier by means of an output device connected thereto. The electronic information carrier includes a CPU generating a second self-checking encryption code having any encryption depth by means of a second algorithm for encrypting all the products being paid. The second encryption code may be different from the first encryption code. The electronic information carrier is supplied to a reading unit in said product delivery storage in order to identify and to decrypt said second encryption code. In case of an authorized identification the delivery of the selected product in the selected quantity from the product delivery storage is started.

The advantages achieved by the invention in particular consist in that a product sale is preferably performed with at least two information carriers which are independent with respect to their storage form so that a secure authorized product delivery is ensured.

In this case, the desired product is selected by a customer at an electronic product delivery terminal arranged within a product offering zone. By means of a printing device associated to the product selection terminal a document serving as an information carrier is output representing the selected product in plain writing for the customer and at the same time comprising a coded and self-checking encryption which is to be decoded by a document reader.

After the payment of the product in a counter zone an electronic information carrier is output to the customer by means of an output device arranged in the immediate vicinity of the counter.

This information carrier may be embodied as a transponder, as a coin-like chip or as a chip card, i.e. a smart card. In one embodiment, the information carrier includes a computing device (CPU) which automatically generates a self-checking encryption encoded by an algorithm

In another case, the delivery means includes a computing device (CPU) for generating the encryption code, this code is then stored in an information carrier arranged as a passive memory which may be_protected against undesired reading by means of a multi-digit PIN.

The information carrier together with the encrypted product data is supplied to a reading unit contained in a product delivery storage arranged outside of the product offering zone for decoding. After a plausibility check by means of the corresponding algorithm f_2, f_2, the decryption arranges for the delivery of the selected product from a product delivery storage.

The information carrier remains in the product delivery storage and, after its recirculation to the counter zone, may be provided at any time with a new encryption.

Further, the product delivery from the product delivery storage is advantageous in that when additional security checks are required, for example, if alcohol or cigarettes are delivered according to the regulations for the legal protection for children and young persons, the product delivery may be performed by an authorized supervisor. As a result, for example, an identity check may be shifted from the counter staff to the security staff.

Further, since the product is coded an authorization check may already be included in the operation of selection at the product selection terminal.

Advantageously, the method especially applies for counter zones in which the customer already can perform himself the identification of the product for the payment operation.

Further, a coded data transmission by means of a wireless or a wired data transmission may advantageously be employed between the product delivery storage and the product selection terminal, in order to protect it against an external data manipulation (hacker attack).

DESCRIPTION OF THE DRAWINGS

An embodiment of the invention is shown in the drawings and is further explained below. In the drawings:

FIG. 1 shows a diagrammatic view of the method for secure data transmission in selling products; and

FIG. 2 shows an explanation of the encryption method.

DETAILED DESCRIPTION OF THE INVENTION

In FIG. 1 the method for secure data transmission in selling products is shown in a diagrammatic view.

In a typical store, the selling zone may be divided into three zones: a product offering zone 1, a counter zone 2 and a product delivery zone 3.

Various products are selected by means of a product selection terminal 10, which is placed within the product offering zone 1. A document printer 14 is connected to the product selection terminal 10 to output a document 16 i.e. a receipt.

The product selection terminal 10 is electronically connected to one or more product delivery storages 30 arranged in the product delivery zone 2.

The document 16 serving as an information carrier contains the selected product in plain writing as well as a code related at least to the sort and the quantity of the product. The code is possibly formed by a random number and by a self-checking number P and an algorithm f_1, respectively; this number is generated and output by a computing device CPU 12 provided at the product selection terminal 10.

In this case, the product identification and also the sale identification of a selling operation may be used for encoding.

The document may be output in paper form and is identified and read by a document reader 22 contained in the counter means 20 when the product offering zone 1 is left and the product delivery zone 2 is entered.

After paying for this product, or even after paying for further products not ordered by means of the product selection terminal, by cash or cashless payment, a delivery means 24 arranged in the counter zone 2 outputs a further information carrier 26. This information carrier contains its own CPU 28 and automatically performing an encryption of the paid products by means of a self-checking number P' and an algorithm f'_1, f'_2.

The information carrier 26 may be embodied as a transponder, as a single chip or as a chip card (smart card).

In a variation, the delivery unit 24 may contain a CPU 28' and perform an encryption, this data is then transmitted to an information carrier 26' arranged as a passive memory.

Additionally, the encryption may possibly be provided with a multi-digit PIN.

In the product delivery zone 3, the information carrier 26, 26' is supplied to a reading unit 32 of the product delivery storage 30. The reading unit 32 decodes the encrypted information and initiates the delivery of the selected products 40.

The information carriers remain in the product delivery storage until they are used again.

In this example, a method is described in which at least two independent encryption methods are used, however, this is not absolutely necessary, since each encryption method may also be employed individually.

An explanation is now given with respect to the method for processing and validating the self-checking data with the help of a self-checking number P_i containing information about the purchase and the authorization with respect to the sort and the quantity of the selected product in view of the delivery at the delivery means 30 and the possibility of coding a logical sequence in a determined portion of the contained digits.

Method:

The encryption process used in the self-checking and the authorization-checking of the operator (final customer), applies the one computation rule (algorithm f_2), and the one computation rule transfers the number X_1 consisting of m digits into the number Y_1 which preferably, but not necessarily, also consists of m digits.

This encryption as well as the checking method for establishing the authenticity of the document may by performed at the product selection terminal by means of a self-checking number P, and at the delivery apparatus in the counter zone with the information carrier 28 embodied as a chip card by means of the self-checking number P'.

It is not relevant whether the algorithms are each the same (f_1 and f_2) or different (f'_1 and f'_2, with $f'_1 \neq f_1$ and f'_2, with $f'_2 \neq f_2$). For the self-checking operation a difference between these two algorithms is not absolutely necessary.

As shown in FIG. 2, the two sets of digits of the number X_1 and the number Y_1, respectively, together compose the desired self-checking encryption number P_1 (and P'_1, respectively).

The encryption algorithm f (i.e. f_1, f_2, f'_1, f'_2) may be any known algorithm. In particular, each known encryption algorithm, for example DES(-RSA), Rijndael, Elliptic Curves or the like or even each newly developed encryption algorithm may be used in this case as far as it is unambiguous with respect to the number Y_1 computed from the number X_1 applied to the input. Thus, if the encryption algorithm composes the desired self-checking encryption number P_1, for example, by "composing" the digits in the order "XY" or possibly if it converts the composition to the desired number by a further computation. X then possibly contains the high-order digits and Y contains the low-order digits of the number P. However, the inverted order (X=low-order digits/Y=high-order digits) is conceivable. The number of digits m has to be selected sufficiently high with respect to the base of the figures.

Preferably, 20 digits would be used by the encryption, but more or less digits may be provided within the scope of the encryption depth if using figures and alphanumeric characters (A-Z; a-z) and special characters. Here, "may be provided" in the sense of the information technology means the number of the used "bits per character" of the used digit, which is in particular used to ensure sufficient security against "lucky shots". Thus, the term "number" is merely a "wild card symbol" for each applicable information unit in the mathematical sense.

Plausibility check algorithm f_1 checks between the generated sale information units in the sense of the "continued sequence" plausibility ("Fortfolge"-Plausibilität):

Further, a second encryption function f_2 is generated which is independent from the first with respect to the algorithm (or possibly even identical) and which exclusively generates a subsequent number X_2 from an input number X_1. Moreover, a number X_3 may be formed from the number X_2 by performing another encryption. The sequence A of numbers produced is a biunique and reproducible sequence A. This sequence serves with each of its individual values as an argument X_i of the subsequent function f_2 in order to generate the above-desired number P_i.

Thus, only a part of the used digits within this number X_i may or must be used for the plausibility check with respect to the number $X_{(i-1)}$ with the help of the algorithm f_1.

The purpose of the plausibility check is to stop fraud. A customer might try to copy the information carrier i.e. the document and use it to obtain multiple products. That is, the potential thief might take the information carrier and reproduce it after leaving the counter and obtain multiple copies of the product using the forged documents. While this type of fraud is difficult, it is not technologically impossible so the plausibility check is necessary.

The uniqueness of the information relevant for the sale contained in the CPU 28 within the scope of the continued sequence of the secret algorithm f_1, f_2 is thus an essential component of this method and cannot be separated therefrom.

The reproducibility of the continued sequence A generated by the secret algorithm f_1 at the relevant digits is thus also a relevant component of the method and cannot be separated therefrom.

Possibilities of storing information within the number X:

A further part of the digits of the corresponding number X_i may or must be used to receive the information about the selected product and the selected quantity of this product, and possibly to receive additional information such as the legal protection for children and young persons. However, it is not necessary to include these further digits in the plausibility check

In this case, it is not necessary, even though not unconceivable and thus also applicable, that the information which is not relevant for the performance and checking operation by the algorithm f_1 (f'_1) is encrypted again. However, this information may be represented in plain writing as indicated in the example.

Further, there is no absolute instruction concerning the ratio of the number of digits of the information within the number X in proportion to the number of digits of the information of the plausibility check done by the algorithm f_1 (f'_1) for the correct sequence of the numbers X_i, so that this ratio may be anyone in so far as a sufficiently secure use of the plausibility check by the algorithm f_1 (f'_1) remains possible.

It is also conceivable that this method may by applied to fixed quantities and fixed codes of sorts; then, there is no necessity to transmit quantities or codes or any other information, since merely a single product in the number one is to be sold. In this special case even all digits of the number X may completely be used for the plausibility check with respect to the algorithm f_1 (f'_1).

Schemata:

The continued application of this schema leads to the sequence P of check numbers. This schema may universally be described by means of the functions f_1 and f_2 (thus, also by means of f'_1, f'_2):

specially: $Y_1=f_2(X_1)$/generally: $Y_n=f_2(X_n):\rightarrow P_1=\{"X_1Y_1"\}$

specially: $Y_2=f_1(X_1)$/generally: $X_{(n-1)}=f_2(X_n):\rightarrow X_i$

each as an argument for f(x).

As a "starting number" (initial number) X_0 for this scheme may, but does not absolutely have to, exist. The number X_0 may be intentionally selected by the user which, as far it is desired, offers a possibility to ensure the reproducibility of the sequence A of numbers by means of the respective algorithm f in CPU 12 and CPU 28, respectively. Alternatively a random number generated by computer might be used.

When the "starting number" is the same in the generating CPU 12 and in the second checking CPU 28 and in each further CPU, then a simple further security function within the scope of a "plausibility check" may be realized.

The same starting numbers lead to the same sequences A of numbers if the algorithms are the same, and thus to the same sequence P of check numbers within the scope of the above-mentioned relevant digits of the sequence $A(X_i)$ of numbers, but it is understood that it is exclusively related to the relevant digits used for the plausibility check of the continued sequence according to the algorithm f_1 (f'_1).

In this particularly advantageous embodiment of the invention, the universal possibility to code information with respect to selected quantities and selected sorts of products within the numbers P_i as well as to check the consistency of continued sequences of numbers is provided if the initial number ("starting number") in all CPU instances within the sequence A of numbers is the same.

Assuming that the initial number is the same in all CPU's, each uniquely generated document and information carrier, respectively, which is generated in the CPU 12 as well as in the information carrier CPU 28, may be generated and also used only one time in this form for selling.